CLAIMS

What is claimed is:

1. A method of preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, the method comprising the computer-implemented steps of:

receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP header is set;

determining whether a sequence value in the packet is within a range of allowed sequence values; and

when the sequence value is within the range of allowed sequence values, sending an acknowledgment message without closing a TCP connection associated with the flow.

2. A method as recited in Claim 1, further comprising the steps of:

receiving, from the remote end node, a next packet of a flow in which the RST bit is set and comprising a second sequence value;

determining whether the second sequence value is equal to an expected sequence value; and

closing a TCP connection associated with the flow only when the second sequence value is equal to the expected sequence value.

3. A method as recited in Claim 1, wherein the range of allowed sequence values does not include the expected sequence value.

4. A method of preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, the method comprising the computer-implemented steps of:

receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP header is set; and

sending an acknowledgment message without closing a TCP connection associated with the flow and without regard to whether a sequence value in the packet is within a range of allowed sequence values.

5. A method as recited in Claim 4, further comprising the steps of:
setting a flag representing receipt of the packet with RST bit set;
receiving, from the remote end node, a next packet of a flow in which the RST bit is set and comprising a sequence value;
determining whether the sequence value equals an expected sequence value; and
closing the TCP connection only when the sequence value equals the expected sequence value.

6. A method as recited in Claim 5, further comprising the step of dropping the packet and the next packet when the RST bit is set and the sequence value of the next packet does not equal an expected sequence value.

7. A method as recited in Claim 4 or Claim 5, further comprising the steps of determining that the RST bit is not set in the packet or the RST bit is set and holds an incorrect sequence number, and in response thereto, clearing the flag.

8. A method as recited in Claim 1, further comprising the steps of accumulating a counter that counts spurious TCP RST packets.

9. A method as recited in Claim 1 or Claim 8, further comprising the steps of generating a notification message when the packet is not successfully validated.

10. A method as recited in any of Claims 1, 2, 3, 4, 5, 6, or 8, further comprising the steps of generating a notification message when either the sequence value or the second sequence value is not within the allowed range of sequence values.

11. A method of preventing an attack on a network, the method comprising the computer-implemented steps of:

receiving, from a remote end node, a packet of a flow in which a SYN bit of a header is set;

sending an acknowledgment message without closing a TCP connection associated with the flow and without regard to whether a sequence value in the packet is within a range of allowed sequence values;

receiving a next packet of the flow; and

when the next packet is a TCP RST packet, performing the steps of Claim 1 or Claim 4 with respect to the next packet.

12. A method as recited in Claim 11, further comprising the steps of taking no action with respect to the TCP connection when the next packet is not a TCP RST packet.

13. A method as recited in Claim 11, further comprising the steps of accumulating a counter that counts spurious TCP SYN packets.

14. A method as recited in any of Claims 11, 12, or 13, further comprising the steps of generating a notification message when the packet is not successfully validated.

15. A method as recited in any of Claims 1, 4, or 11, wherein the steps are performed by a router or switch in a packet-switched network.

16. A method of preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, the method comprising the computer-implemented steps of:

receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP header is set; and

determining whether a sequence value in the packet is within a range of allowed sequence values including the expected sequence value; and

when the sequence value is within the range of allowed sequence values including the expected value, sending an acknowledgment message without closing a TCP connection associated with the flow.

17. A method as recited in Claim 18, further comprising the steps of:
setting a flag representing receipt of the packet with RST bit set;
receiving, from the remote end node, a next packet of a flow in which the RST bit is set and comprising a sequence value;
determining whether the sequence value equals an expected sequence value; and
closing the TCP connection only when the sequence value equals the expected sequence value.

18. A method as recited in Claim 17, further comprising the step of dropping the packet and the next packet when the RST bit is set and the sequence value of the next packet does not equal an expected sequence value.

19. A method as recited in Claim 16 or Claim 17, further comprising the steps of determining that the RST bit is not set or the RST bit is set and hold the incorrect sequence number in the next packet, and in response thereto, clearing the flag.

20. An apparatus for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, comprising:
means for receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP header is set;
means for determining whether a sequence value in the packet is within a range of allowed sequence values; and
means for sending, when the sequence value is within the range of allowed sequence values, an acknowledgment message without closing a TCP connection associated with the flow.

21. An apparatus for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, comprising:

a processor;

one or more stored sequences of instructions that are accessible to the processor and which, when executed by the processor, cause the processor to carry out the steps of:

receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP header is set;

determining whether a sequence value in the packet is within a range of allowed sequence values; and

when the sequence value is within the range of allowed sequence values, sending an acknowledgment message without closing a TCP connection associated with the flow.

22. A computer-readable medium carrying one or more sequences of instructions for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, wherein the execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP header is set;

determining whether a sequence value in the packet is within a range of allowed sequence values; and

when the sequence value is within the range of allowed sequence values, sending an acknowledgment message without closing a TCP connection associated with the flow.

23. An apparatus for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, comprising:

means for receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP header is set; and

means for sending an acknowledgment message without closing a TCP connection associated with the flow and without regard to whether a sequence value in the packet is within a range of allowed sequence values.

24. An apparatus for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, comprising:

a processor;

one or more stored sequences of instructions that are accessible to the processor and which, when executed by the processor, cause the processor to carry out the steps of:

receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP header is set; and

sending an acknowledgment message without closing a TCP connection associated with the flow and without regard to whether a sequence value in the packet is within a range of allowed sequence values

25. A computer-readable medium carrying one or more sequences of instructions for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, wherein the execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP header is set; and

sending an acknowledgment message without closing a TCP connection associated with the flow and without regard to whether a sequence value in the packet is within a range of allowed sequence values.

26. An apparatus for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, comprising:

means for receiving, from a remote end node, a packet of a flow in which a SYN bit of a header is set;

means for sending an acknowledgment message without closing a TCP connection associated with the flow and without regard to whether a sequence value in the packet is within a range of allowed sequence values;

means for receiving a next packet of the flow; and

means for performing the functions provided by the means of Claim 20 or Claim 23 when the next packet is a TCP RST packet.

27. An apparatus for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, comprising:

a processor;

one or more stored sequences of instructions that are accessible to the processor and which, when executed by the processor, cause the processor to carry out the steps of:

receiving, from a remote end node, a packet of a flow in which a SYN bit of a header is set;

sending an acknowledgment message without closing a TCP connection associated with the flow and without regard to whether a sequence value in the packet is within a range of allowed sequence values;

receiving a next packet of the flow; and

when the next packet is a TCP RST packet, performing the steps of Claim 1 or Claim 4 with respect to the next packet.

28. A computer-readable medium carrying one or more sequences of instructions for preventing an attack on a network, wherein the attack comprises sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, wherein the execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

receiving, from a remote end node, a packet of a flow in which a SYN bit of a header is set;

sending an acknowledgment message without closing a TCP connection associated with the flow and without regard to whether a sequence value in the packet is within a range of allowed sequence values;

receiving a next packet of the flow; and

when the next packet is a TCP RST packet, performing the steps of Claim 1 or Claim 4 with respect to the next packet.